Security

How we help protect your information

We take our responsibility to safeguard your information very seriously and employ safeguards in order to help insure that your information is protected as it is transmitted from your computer and stored on our computers at Liberty Insurance Singapore.

Encryption

When dealing with your personal/private information on our computers, and working in partnership with your browser, use an industry standard security protocol (Secure Sockets Layer – SSL) to help ensure that the information is encrypted and protected from eavesdropping. SSL helps insure that the conversation your browser is having with our servers is private and that the information contained therein is safe and delivered only to our computers.

Firewall

Once your information reaches our servers we protect it in many ways including storing the information on secure servers and using a device known as a firewall which protects your information by detecting and preventing un-authorized access to the information.

Authorized access

We protect your information by only allowing access to your information by employees and with authorized parties who have a legitimate and verified need to access the information in order to service your requests.

Passwords

- Password should not be based on user-id, personal telephone number, birthday or other personal information.
- Password must be kept confidential and not be divulged to anyone.
- Password must be memorized and not be recorded anywhere.
- Password should be changed regularly.
- The same Password should not be used for different websites, applications or services, particularly when they relate to different entities.
- Not advisable to select the browser option for storing or retaining user name and password.

Safer Internet Usage

We recommend to

- Maintain your computer current with latest Operating System (OS) patches installed
- Install a personal firewall and anti-virus software and update them regularly
- Use latest version of the browser to protect your system from malware and viruses.
- Remove file and printer sharing in their computers, especially when they have internet access via cable modems, broadband connections or similar set-ups.
- Check the authenticity of the financial institution's website by comparing the URL and the financial institution's name in its digital certificate or by observing the indicators provided by an extended validation certificate.

- Check that the financial institution's website address changes from http:// to https:// and a security icon that looks like a lock or key appears when authentication and encryption is expected.
- Do not use public or internet café computers to access online portal and perform financial transactions.

Good Practices

Do's

- Make regular backup of critical data.
- Consider the use of encryption technology to protect highly sensitive data stored in your personal computer.
- Log off the online session and turn off the computer when not in use.
- Delete junk or chain emails.

Don'ts

- Do not install software or run programs of unknown origin.
- Do not open email attachments from strangers.
- Do not disclose personal, financial or credit card information to little-known or suspect websites.
- Do not use a computer or a device which cannot be trusted.